Docket No.: 2565-0297PUS1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Takehiro OHKOSHI et al.

Application No.: 10/584,194

Confirmation No.: 1262

Filed: May 25, 2007

Art Unit: 2431

For: AUTHENTICATED DEVICE, AUTHENTICATING DEVICE AND AUTHENTICATING METHOD

Examiner: K. Abrishamkar

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As required under § 41.37(a), this brief is filed within one month from the Notice of Panel Decision dated September 4, 2009.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.2:

I.	Real Party In Interest
II	Related Appeals and Interferences
III.	Status of Claims
IV.	Status of Amendments
V.	Summary of Claimed Subject Matter
VI.	Grounds of Rejection to be Reviewed on Appeal
VII.	Argument
VIII.	Conclusion

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

MITSUBISHI ELECTRIC CORPORATION
7-3, MARUNOUCHI 2-CHOME,CHIYODA-KU
TOKYO, JAPAN 100-8310

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 10 claims pending in application.

B. Current Status of Claims

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-10
4. Claims allowed: none
5. Claims rejected: all pending claims (1-10)

C. Claims On Appeal

The claims on appeal are all pending claims (1-10). Claims 1, 4 and 7-10 are independent.

IV. STATUS OF AMENDMENTS

Appellants did not file an Amendment After Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

With respect to independent claim 1, the claimed invention is directed to an authenticated device (item 200 of Fig. 1). The authenticated device (200) includes a memory unit (item 220 of Fig. 1) to store at least one algorithm identifier and at least one encryption key identifier (lines 1-3, page 11); a transmitting unit (item 212 of Fig. 1) to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit (220) to an authenticating device (item 100 of Fig. 1; lines 18-20, page 12); a receiving unit (item 211 of Fig. 1) to receive from the authenticating device (100) a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit (212; line 21, page 14 to line 5, page 15); and an authentication processing unit (item 296 of Fig. 1) to perform an authentication process with the authenticating device (100), based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit (211; lines 11-14, page 19).

With respect to independent claim 4, the claimed invention is directed to an authenticating device (item 100 of Fig. 1). The authenticating device (100) includes a memory unit (item 120 of Fig. 1) to store at least one algorithm identifier and at least one encryption key identifier (lines 20-22, page 10); a receiving unit (item 111 of Fig. 1) to receive at least one algorithm identifier and at least one encryption key identifier from an authenticated device (200; line 22, page 12 to line 3, page 13); a selecting unit (item 160 of Fig. 1) to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit (120) from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit (111), when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit (120) exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit (111; lines 6-9, page 13); a transmitting unit (item 112 of Fig. 1) to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit (160) to the authenticated device (200; lines 15-20, page 14); and an authentication processing unit (item 196 of Fig. 1) to perform an authentication process with the authenticated device (200), based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit (112; lines 3-6, page 20).

With respect to independent claim 7, the claimed invention is directed to an authenticating method. The authenticating method includes the steps of a first transmitting step to transmit, from an authenticated device (item 200 of Fig. 1) storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device (item 100 of Fig. 1), the plurality of algorithm identifiers and the plurality of encryption key identifiers stored (item S205 of Fig. 2; lines 9 and 10, page 11 and lines 18-21, page 12); a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device (200) by the first transmitting step, at the authenticating device (100) storing at least one algorithm identifier and at least one encryption key identifier (item S206 of Fig. 2; line 22, page 12 to line 3, page 13); a selecting step to select, at the authenticating device (100), a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device (100) from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device (100) exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step (item S207 of Fig. 2; lines 4-9, page 13); a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device (100) to the authenticated device (200; item S211 of Fig. 2; lines 15-20, page 14); a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device (100), at the authenticated device (200; item S212 of Fig. 2; line 21, page 14 to line 1, page 15); and an authentication processing step to perform an authentication process between the authenticating device (100) and the authenticated device (200), based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step (lines 11-14, page 19 and lines 3-6, page 20). See also line 15, page 29 to line 16, page 30.

With respect to claim 8, the claimed invention is directed to an authenticating method. The authenticating method includes the steps of a first transmitting step to transmit, from an authenticated device (item 200 of Fig. 1) storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device (item 100 of Fig. 1), the at least one algorithm identifier and the at least one encryption key identifier stored (item S205 of Fig. 2; lines 18-21, page 12); a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device (200) by the first transmitting step, at the authenticating device (100) storing a plurality of algorithm identifiers and a plurality of encryption key identifiers (item S206 of Fig. 2; lines 9 and 10, page 11 and line 22, page 12 to line 3, page 13); a selecting step to select, at the authenticating device (100), a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device (100) from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device (100) exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step (item S207 of Fig. 2; lines 4-9, page 13); a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device (100) to the authenticated device (200; item S211 of Fig. 2; lines 15-20, page 14); a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device (100), at the authenticated device (200; item S212 of Fig. 2; line 21, page 14 to line 1, page 15); and an authentication processing step to perform an authentication process between the authenticating device (100) and the authenticated device (200), based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step (lines 11-14, page 19 and lines 3-6, page 20). See also line 17, page 30 to line 17, page 31.

With respect to claim 9, the claimed invention is directed to an authenticating method. The authenticating method includes transmitting, from an authenticated device (item 200 of Fig. 1) storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device (item 100 of Fig. 1), the plurality of algorithm identifiers and the plurality of encryption key identifiers stored (lines 9 and 10, page 11 and lines 18-21, page 12); receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device (200), at the authenticating device (100) storing at least one algorithm identifier and at least one encryption key identifier (line 22, page 12 to line 3, page 13); selecting, at the authenticating device (100), a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device (100) from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device (100) exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received (lines 4-9, page 13); transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device (100) to the authenticated device (200; lines 15-20, page 14); receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device (100), at the authenticated device (200; line 21, page 14 to line 1, page 15); and performing an authentication process between the authenticating device (100) and the authenticated device (200), based on the prescribed algorithm identifier and the prescribed encryption key identifier received (lines 11-14, page 19 and lines 3-6, page 20). See also line 15, page 29 to line 16, page 30.

With respect to claim 10, the claimed invention is directed to an authenticating method. The authenticating method includes transmitting, from an authenticated device (item 200 of Fig. 1) storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device (item 100 of fig. 1), the at least one algorithm identifier and the at least one encryption key identifier stored (lines 18-21, page 12); receiving the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device (200), at the authenticating device (100) storing a plurality of algorithm identifiers and a plurality of encryption key identifiers (lines 9 and 10, page 11 and line 22, page 12 to line 3, page 13); selecting, at the authenticating device (100), a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device (100) from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device (100) exist among the at least one algorithm identifier and the at least one encryption key identifier received (lines 4-9, page 13); transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device (100) to the authenticated device (200; lines 15-20, page 14); receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device (100), at the authenticated device (200; line 21, page 14 to line 1, page 15); and performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received (lines 11-14, page 19 and lines 3-6, page 20). See also line 17, page 30 to line 17, page 31.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-10 are properly rejected under 35 USC 102(e) as being anticipated by Edgett et al. (U.S. Patent Publication No. US 2004/0034771; hereinafter "Edgett").

VII. ARGUMENT

Claims 1-10 are not anticipated by Edgett because Edgett fails to disclose each and every claimed element.

In order to support a rejection under 35 U.S.C. § 102, the cited reference must teach each and every claimed element. In the present case, claims 1-10 are not anticipated by Edgett for at least the reason that Edgett fails to disclose each and every claimed element as discussed below.

Independent Claim 1

Appellants respectfully submit that Edgett fails to teach or suggest each and every claimed element of independent claim 1. For example, independent claims 1 recites, *inter alia*,

> a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device;
>
> a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit.

Edgett disclose that when a dialer containing an old algorithm communicates with a network, the dialer encrypts a password using the old algorithm. The encrypted password, a corresponding key index and an associated algorithm identifier are then transmitted to the server. The server then utilizes the algorithm identifier to identify the corresponding algorithm to be used for decrypting the password for authentication. Once the dialer is authenticated and connected to the server, an Update Server determines if an algorithm update is required. If an algorithm update is required, the new algorithm and its associated key identifier are downloaded to the dialer. See paragraphs [0056]-[0059] of Edgett. In other words, the dialer transmits the old algorithm to the server for an authentication process and receives a new algorithm if there is an algorithm update required.

In the Final Rejection dated April 3, 2009 ("Final Rejection"), the Examiner alleges that the new algorithm received by a dialer from a server in Edgett corresponds to "receiv[ing] a prescribed algorithm identifier and a prescribed encryption key identifier, **which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit**" as claimed. See paragraph 2, page 2 of Final Rejection. Appellants respectfully disagree.

The new algorithm and the new corresponding algorithm identifier in Edgett represent a newly developed algorithm and are completely unrelated to the old algorithm and the old corresponding algorithm identifier transmitted by the dialer. See paragraph [0057].

Therefore, contrary to the assertion by the Examiner, the updated key index and algorithm identifier received by the dialer in Edgett are NOT a prescribed algorithm identifier and a prescribed encryption key identifier, **which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit** as claimed. As such, the dialer in Edgett cannot be equated with the claimed authenticated device.

Thus, Edgett fails to disclose or suggest at least "a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit" as claimed.

Dependent Claims 2 and 3

Claims 2 and 3 depend from claim 1. Therefore, for at least the reasons stated with respect to claim 1, claims 2 and 3 are also distinguishable from Edgett.

Independent Claim 4

Appellants respectfully submit that Edgett fails to teach or suggest each and every claimed element of independent claim 4. For example, independent claims 4 recites, *inter alia*,

> a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit;
>
> a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device.

First, the Final Rejection fails to respond to Appellants' arguments with respect independent claim 4. The Final Rejection merely restated that Edgett teaches storing key index and algorithm in a private key database. See pages 6 and 7 of Final Rejection.

Edgett discloses generating a public/private key pair. The public/private key pair is tagged with a key index and algorithm identifier. A dialer customization tool includes the public key, its corresponding key index and the algorithm. The dialer customization tool stores the private key, its corresponding key index and the algorithm identifier in a private key database of a server (38, Fig. 2 and paragraph 58). As such, the dialer is authenticated by the server using the public/private key pair. In other words, the private key database in Edgett merely stores the private key data in a public/private key pair.

However, the stored private key, its corresponding key index and the algorithm identifier in the server of Edgett are NOT a prescribed algorithm identifier and a prescribed encryption key identifier selected to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, **when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit** as claimed. Unlike the present invention, Edgett does not select a prescribed algorithm identifier and a prescribed encryption key identifier based on whether the previously stored algorithm identifier and encryption key identifier exist among the received algorithm identifier and encryption key identifier.

Furthermore, even if, *arguendo*, the algorithm identifier (corresponding to the private key) stored in the private key database/server in Edgett is a prescribed algorithm identifier selected from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, the private key database/server in Edgett still does not transmit **the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to an authenticated device** as claimed. In Edgett, the stored algorithm identifier in the private key database/server is merely for authentication process when a dialer attempting to connect to the server. The stored algorithm identifier in the private key database/server is not transmitted back to the dialer. In addition, contrary to the assertion by the

Examiner, the updated algorithm and algorithm identifier transmitted to the dialer in Edgett represent a newly developed algorithm and are completely unrelated to the old algorithm and algorithm identifier stored in the private key database/server.

Thus, Edgett fails to disclose or suggest at least the above-mentioned features in claim 4.

Dependent Claims 5 and 6

Claims 5 and 6 depend from claim 4. Therefore, for at least the reasons stated with respect to claim 4, claims 5 and 6 are also distinguishable from Edgett.

Independent Claim 7

Appellants respectfully submit that Edgett fails to teach or suggest each and every claimed element of independent claim 7. For example, independent claims 7 recites, *inter alia,*

> a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored;
>
> a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;
>
> a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step;
>
> a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by

> the selecting step, from the authenticating device to the authenticated device;
>
> a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device.

First, the Final Rejection fails to respond to Appellants' arguments with respect independent claim 7.

Edgett is merely concerned with an authentication process between a dialer and a server based on a public/private key pair, a corresponding key index and an algorithm identifier. Once authenticated, if there is an updated key or algorithm, the server then sends the newly developed key or algorithm to the dialer. In other words, a single set of key/algorithm is being sent from dialer to the server during the authentication process. If there is an update required, a single set of key/algorithm is being sent from server to the dialer. Thus, Edgett simply cannot disclose or suggest transmitting and receiving **a plurality of algorithm identifiers and a plurality of encryption key identifiers stored** between an authenticating device and an authenticated device, and selecting a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among **the plurality of algorithm identifiers and the plurality of encryption key identifiers received** as claimed.

Furthermore, Edgett discloses generating a public/private key pair. The public/private key pair is tagged with a key index and algorithm identifier. A dialer customization tool includes the public key, its corresponding key index and the algorithm. The dialer customization tool stores the private key, its corresponding key index and the algorithm identifier in a private key database of a server (38, Fig. 2 and paragraph 58). As such, the dialer is authenticated by the server using the public/private key pair. In other words, the private key database in Edgett merely stores the private key data in a public/private key pair.

However, the stored private key, its corresponding key index and the algorithm identifier in the server of Edgett are NOT a prescribed algorithm identifier and a prescribed encryption key identifier selected to be stored by the authenticating device **from among the plurality of algorithm identifier and the plurality encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored exist among**

the at plurality algorithm identifiers and the plurality encryption key identifiers received as claimed. Unlike the present invention, Edgett does not select a prescribed algorithm identifier and a prescribed encryption key identifier based on whether the previously stored algorithm identifier and encryption key identifier exist among the received algorithm identifiers and encryption key identifiers.

Furthermore, even if, *arguendo*, the algorithm identifier (corresponding to the private key) stored in the private key database/server of Edgett is a prescribed algorithm identifier selected from among the plurality algorithm identifiers and the plurality encryption key identifiers received, the private key database/server in Edgett still does not transmit **the prescribed algorithm identifier and the prescribed encryption key identifier selected from an authenticating device to an authenticated device** as claimed. In Edgett, the stored algorithm identifier in the private key database/server is merely for authentication process when a dialer attempting to connect to the server. The stored algorithm identifier in the private key database/server is not transmitted back to the dialer. In addition, contrary to the assertion by the Examiner, the updated algorithm and algorithm identifier transmitted to the dialer in Edgett represent a newly developed algorithm and are completely unrelated to the old algorithm and algorithm identifier stored in the private key database/server.

Thus, Edgett fails to disclose or suggest at least the above-mentioned features in claim 7.

Independent Claim 8

Appellants respectfully submit that Edgett fails to teach or suggest each and every claimed element of independent claim 8. For example, independent claims 8 recites, *inter alia,*

> a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step;

> a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device;

First, the Final Rejection fails to respond to Appellants' arguments with respect independent claim 8.

Edgett discloses generating a public/private key pair. The public/private key pair is tagged with a key index and algorithm identifier. A dialer customization tool includes the public key, its corresponding key index and the algorithm. The dialer customization tool stores the private key, its corresponding key index and the algorithm identifier in a private key database of a server (38, Fig. 2 and paragraph 58). As such, the dialer is authenticated by the server using the public/private key pair. In other words, the private key database in Edgett merely stores the private key data in a public/private key pair.

However, the stored private key, its corresponding key index and the algorithm identifier in the server of Edgett are NOT a prescribed algorithm identifier and a prescribed encryption key identifier selected to be stored from among the at least one algorithm identifier and the at least one encryption key identifier received, **when the at least one of plurality algorithm identifiers and the at least one of plurality encryption key identifiers stored exist among the at least one algorithm identifier and the at least one encryption key identifier received** as claimed. Unlike the present invention, Edgett does not select a prescribed algorithm identifier and a prescribed encryption key identifier based on whether the previously stored algorithm identifier and encryption key identifier exist among the received algorithm identifier and encryption key identifier.

Furthermore, even if, *arguendo*, the algorithm identifier (corresponding to the private key) stored in the private key database/server in Edgett is a prescribed algorithm identifier selected from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, the private key database/server in Edgett still does not transmit **the prescribed algorithm identifier and the prescribed encryption key identifier selected from an authenticating to an authenticated device** as claimed. In Edgett, the stored algorithm identifier in the private key database/server is merely for authentication process when a dialer attempting to connect to the server. The stored algorithm identifier in the private key database/server is not transmitted back to the dialer. In addition, contrary to the assertion by the Examiner, the updated algorithm and algorithm identifier transmitted to the dialer in Edgett represent a newly developed algorithm and are completely unrelated to the old algorithm and algorithm identifier stored in the private key database/server.

Thus, Edgett fails to disclose or suggest at least the above-mentioned features in claim 8.

Independent Claim 9

Appellants respectfully submit that Edgett fails to teach or suggest each and every claimed element of independent claim 9. For example, independent claims 7 recites, *inter alia*,

> transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored;
>
> receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;
>
> selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received;
>
> transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device;
>
> receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device.

First, the Final Rejection fails to respond to Appellants' arguments with respect independent claim 9.

Edgett is merely concerned with an authentication process between a dialer and a server based on a public/private key pair, a corresponding key index and an algorithm identifier. Once authenticated, if there is an updated key or algorithm, the server then sends the newly developed key or algorithm to the dialer. In other words, a single set of key/algorithm is being sent from dialer to the server during the authentication process. If there is an update required, a single set of key/algorithm is being sent from server to the dialer. Thus, Edgett simply cannot disclose or suggest transmitting and receiving **a plurality of algorithm identifiers and a plurality of encryption key identifiers stored** between an authenticating device and an authenticated device, and selecting a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among **the plurality of algorithm identifiers and the plurality of encryption key identifiers received** as claimed.

Furthermore, Edgett discloses generating a public/private key pair. The public/private key pair is tagged with a key index and algorithm identifier. A dialer customization tool includes the public key, its corresponding key index and the algorithm. The dialer customization tool stores the private key, its corresponding key index and the algorithm identifier in a private key database of a server (38, Fig. 2 and paragraph 58). As such, the dialer is authenticated by the server using the public/private key pair. In other words, the private key database in Edgett merely stores the private key data in a public/private key pair.

However, the stored private key, its corresponding key index and the algorithm identifier in the server of Edgett are NOT a prescribed algorithm identifier and a prescribed encryption key identifier selected to be stored by the authenticating device **from among the plurality of algorithm identifier and the plurality encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored exist among the at plurality algorithm identifiers and the plurality encryption key identifiers received** as claimed. Unlike the present invention, Edgett does not select a prescribed algorithm identifier and a prescribed encryption key identifier based on whether the previously stored algorithm identifier and encryption key identifier exist among the received algorithm identifiers and encryption key identifiers.

Furthermore, even if, *arguendo*, the algorithm identifier (corresponding to the private key) stored in the private key database/server of Edgett is a prescribed algorithm identifier selected from among the plurality algorithm identifiers and the plurality encryption key identifiers received, the private key database/server in Edgett still does not transmit **the prescribed algorithm identifier and the prescribed encryption key identifier selected from an authenticating device to an authenticated device** as claimed. In Edgett, the stored algorithm identifier in the private key database/server is merely for authentication process when a dialer attempting to connect to the server. The stored algorithm identifier in the private key database/server is not transmitted back to the dialer. In addition, contrary to the assertion by the Examiner, the updated algorithm and algorithm identifier transmitted to the dialer in Edgett represent a newly developed algorithm and are completely unrelated to the old algorithm and algorithm identifier stored in the private key database/server.

Thus, Edgett fails to disclose or suggest at least the above-mentioned features in claim 9.

Independent Claim 10

Appellants respectfully submit that Edgett fails to teach or suggest each and every claimed element of independent claim 10. For example, independent claims 10 recites, *inter alia*,

> selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received;
>
> transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device;

> receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device

First, the Final Rejection fails to respond to Appellants' arguments with respect independent claim 10.

Edgett discloses generating a public/private key pair. The public/private key pair is tagged with a key index and algorithm identifier. A dialer customization tool includes the public key, its corresponding key index and the algorithm. The dialer customization tool stores the private key, its corresponding key index and the algorithm identifier in a private key database of a server (38, Fig. 2 and paragraph 58). As such, the dialer is authenticated by the server using the public/private key pair. In other words, the private key database in Edgett merely stores the private key data in a public/private key pair.

However, the stored private key, its corresponding key index and the algorithm identifier in the server of Edgett are NOT a prescribed algorithm identifier and a prescribed encryption key identifier selected to be stored from among the at least one algorithm identifier and the at least one encryption key identifier received, **when the at least one of plurality algorithm identifiers and the at least one of plurality encryption key identifiers stored exist among the at least one algorithm identifier and the at least one encryption key identifier received** as claimed. Unlike the present invention, Edgett does not select a prescribed algorithm identifier and a prescribed encryption key identifier based on whether the previously stored algorithm identifier and encryption key identifier exist among the received algorithm identifiers and encryption key identifiers.

Furthermore, even if, *arguendo*, the algorithm identifier (corresponding to the private key) stored in the private key database/server in Edgett is a prescribed algorithm identifier selected from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, the private key database/server in Edgett still does not transmit **the prescribed algorithm identifier and the prescribed encryption key identifier selected from an authenticating to an authenticated device** as claimed. In Edgett, the stored algorithm identifier in the private key database/server is merely for authentication process when a dialer attempting to connect to the server. The stored algorithm identifier in the private key database/server is not transmitted back to the dialer. In addition, contrary to the assertion by the Examiner, the updated algorithm and algorithm identifier transmitted to the dialer in Edgett represent a newly developed algorithm and are completely unrelated to the old algorithm and algorithm identifier stored in the private key database/server.

Thus, Edgett fails to disclose or suggest at least the above-mentioned features in claim 10.

VIII. CONCLUSION

The withdrawal of the outstanding rejections and the allowance of claims 1-10 are earnestly solicited.

IX. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

X. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

XI. RELATED PROCEEDINGS

No related proceedings are referenced in II. above, or copies of decisions in related proceedings are not provided, hence no Appendix is included.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required by this paper and to credit any overpayment to Deposit Account No. 02-2448.

Dated: October 5, 2009

Respectfully submitted,

By

D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 10/584,194

1. (Original) An authenticated device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier;

a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device;

a receiving unit to receive from the authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit; and

an authentication processing unit to perform an authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit.

2. (Original) The authenticated device of claim 1,

wherein the memory unit stores at least one algorithm identifier and at least one encryption key identifier in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile;

wherein the transmitting unit transmits, to the authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile;

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier paired as a prescribed profile, among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit; and wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired as the prescribed profile received by the receiving unit.

3. (Original) The authenticated device of claim 2,

wherein the memory unit further stores a version identifier to identify a version indicating a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored;

wherein the transmitting unit transmits the version identifier stored by the memory unit to the authenticating device;

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier corresponding to a prescribed algorithm among the at least one algorithm forming the set indicated by the version identified by the version identifier transmitted from the transmitting unit; and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier received by the receiving unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier.

4. (Original) An authenticating device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier;

a receiving unit to receive at least one algorithm identifier and at least one encryption key identifier from an authenticated device;

a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit;

a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device; and

an authentication processing unit to perform an authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit.

5. (Original) The authenticating device of claim 4,

wherein the memory unit stores at least one profile identifier to identify at least one profile, whereby one algorithm identifier among the at least one algorithm identifier and one encryption key identifier among the at least one encryption key identifier are paired;

wherein the receiving unit further receives at least one profile identifier from the authenticated device;

wherein the selecting unit selects a prescribed profile identifier to be stored by the memory unit from among the at least one profile identifier received by the receiving unit, when the at least one profile identifier stored by the memory unit exists among the at least one profile identifier received by the receiving unit;

wherein the transmitting unit transmits the prescribed profile identifier selected by the selecting unit to the authenticated device; and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired by a prescribed profile identified by the prescribed profile identifier transmitted by the transmitting unit.

6. (Original) The authenticating device of claim 5,

wherein the memory unit further stores a version identifier to identify a version of a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored;

wherein the receiving unit further receives a prescribed version identifier from the authenticated device;

wherein the selecting unit selects the prescribed algorithm identifier corresponding to one algorithm in the set indicated by the version identified by the prescribed version identifier received by the receiving unit;

wherein the transmitting unit transmits the prescribed algorithm identifier selected by the selecting unit to the authenticated device; and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier transmitted by the transmitting unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier.

7. (Original) An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored;

a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step;

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device;

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device; and an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step.

8. (Original) An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored;

a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device by the first transmitting step, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers;

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step;

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device;

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device; and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step.

9. (Original) An authenticating method comprising:

transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored;

receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received;

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device; and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received.

10. (Original) An authenticating method comprising:

transmitting, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored;

receiving the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers;

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received;

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device; and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received.

APPENDIX B

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

APPENDIX C

No related proceedings are referenced in II. above, hence copies of decisions in related proceedings are not provided.